A Survey of Self-Protecting Computing Systems

Essien Ayanam
The Volgenau School of Engineering
George Mason University
Fairfax, Virginia, 22030, USA
Email: eayanam@gmu.edu
Outline

- Introduction
- Overview
- Classifications
- Critiques
- Related Work
- Conclusion
Introduction

- Autonomic Computing – implementing technology to install, configure, optimize, and manage technology
- Four key areas to autonomic computing – self-configuration, self-optimization, self-healing and self-protection
- These key areas are the foundation of autonomic computing
## Introduction

<table>
<thead>
<tr>
<th>Area</th>
<th>Summarization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Configuration</td>
<td>An automated configuration of components and systems based on provided high-level policies. The rest of the system adjusts seamlessly and automatically.</td>
</tr>
<tr>
<td>Self-Optimization</td>
<td>A system continually seeks opportunities to improve its own performance and efficiency.</td>
</tr>
<tr>
<td>Self-Healing</td>
<td>A system automatically detects, diagnoses, and repairs localized software and hardware problems.</td>
</tr>
<tr>
<td>Self-Protection</td>
<td>A system automatically defends against malicious attacks or cascading failures. It uses early warning to anticipate and prevent system wide failures.</td>
</tr>
</tbody>
</table>
Introduction

- Self Protection/Self Protecting Systems
  - Reactive Security Mechanism: Detects an attack on occurrence and automatically mitigates the attack
  - Proactive Security Mechanism: Anticipate an attack based on current system configuration and learned security occurrences and takes steps to mitigate any potential issues
- Ultimate goal – autonomic security system to operate in a proactive manner
Overview

- Six approaches were surveyed
- Range of topics covering a diverse set of security mechanisms
- Based on their security properties and approach, the mechanisms can be classified as such:
  - Architecture
  - Controller
  - Wireless
Classification

- Autonomic Computing
  - Self-Configuration
  - Self-Optimization
  - Self-Healing
  - Self-Protection

- Architecture
- Controller
- Wireless
Classification - Architecture

- Employ security mechanisms that protect the system as a whole
- Approach security in terms of a layered approach
- Effective in employing repeatable methods to allow for construction of dynamic software

- Proposed an architecture-based self protection (ABSP) approach
- Detection and mitigation of security threats are informed by an architectural representation of the software
- Employs architecture-level self protection patterns to solve well-known security threats
Classification - Architecture

- Virtual Environments Self-Protecting Architecture (VESPA) – self protection for cloud based infrastructures
- Regulates protection of IaaS resources through coordinated security loops
- Enforce granular policies that address multi-layered defense
Ensure optimal system performance while attempting to satisfy conflicting requirements – QoS and Security

Controller optimizes a global utility function

Solution employs combinatorial search techniques and queuing network models to dynamically search for a near-optimal security configuration
Classification - Controller


Classification - Controller

- Implement autonomic system capabilities that can integrate both security and QoS requirements in database applications
- Dynamically changes security configurations according to certain workload characteristics
- Implement Intrusion Detection and Prevention System mechanisms to properly secure the system while meeting QoS requirements and maintaining optimal system performance
- Implement a controller in a TPC-W e-commerce – a transactional web commerce benchmark that emulates the operation of an online bookstore
Classification - Wireless

- Implements a general purpose wireless self-protection system that addresses the overall wireless architecture or implement a system that addresses a specific layer of the network
- Accounts for multiple differing technologies (WPAN, WLAN, WRAN, etc.)
- Provide a comprehensive security strategy for a diverse wireless infrastructure
Classification - Wireless


- Self-protect against attacks by online monitoring and analyzing anomalies and misuses in the network features

- Overall WSPS architecture that provides a comprehensive security strategy for a diverse wireless infrastructure
Classification - Wireless

- Provides a solution to protect the network layer in a mobile ad hoc network
- Protects both routing and packet forwarding functionalities
- Exploits collaboration among local nodes to protect the network layer without completely trust any individual node
Critiques

- Architecture Type Self-Protecting Systems
  - Positives
    - Well written and organized
    - Excellent job in providing the challenges and addressing the challenges via the proposed architecture
  - Negatives
    - Exclusion of pertinent information due to space limitation
    - Expansion on experimental results
Critiques

- Controller Type Self-Protecting Systems
  - Positives
    - Well researched and comprehensive
    - Provided detailed information in identifying the components of the architecture
  - Suggestions
    - Use of actual IDPSs and DB data
    - Implement the controller in a SANs environment
Critiques

- Wireless Type Self-Protecting Systems
  - Positives
    - Innovative solutions
    - Excellent job in providing the challenges and addressing the challenges via the proposed architecture
  - Negatives
    - Poorly completed research study
    - Incomplete research study – missing experimental evaluation
Conclusion

- Comprehensive survey on a number of past and ongoing research efforts on self-protecting computing systems
- Proposal of a new classification for self-protecting systems
- Increased need for additional study in this area through future research
- Limitation – limited number of self-protecting approaches; advantageous to show an effective classification by increasing the scope of the surveys
- Future research – expand scope of self-protecting mechanisms; incorporating the components of from two of the proposed classification to create a new self-protecting mechanism (Architecture and Controller)